УДК 004.4

Жаббаров Ж.К.

Магистрант

Ташкентский университет информационных технологий

Узбекистан, Ташкент

Садиков Р.Т

преподаватель PhD

Ташкентский университет информационных технологий

Узбекистан, Ташкент

ПРАКТИЧЕСКОЕ ВНЕДРЕНИЕ ДОМЕННОЙ ИНФРАСТРУКТУРЫ ДЛЯ ПРЕДПРИЯТИЯ: ОТ ПОДГОТОВКИ СЕРВЕРНОЙ СРЕДЫ ДО ОПТИМИЗАЦИИ БЕЗОПАСНОСТИ

Аннотация: *В данной статье рассматривается комплексный процесс практического внедрения доменной инфраструктуры для предприятий и организаций. Представлены этапы подготовки серверной среды, установки и настройки Domain Controller, интеграции служб DNS и DHCP, а также создания учётных записей пользователей и настройки политик безопасности. Особое внимание уделено таким аспектам, как резервное копирование и восстановление, многоуровневая защита (Defense-in-Depth), модель Tiered Administration и централизованное управление безопасностью через Group Policy. Результаты исследования могут быть применены при проектировании и развёртывании доменной инфраструктуры в средних и крупных организациях.*

Ключевые слова: *доменная инфраструктура, Active Directory, Domain Controller, Group Policy, безопасность, DNS, DHCP, резервное копирование*

Jabborov J.K.

Master's student

Tashkent University of Information Technologies

Uzbekistan, Tashkent

Sadikov R.T

O‘qituvchi PhD

Tashkent University of Information Technologies

Uzbekistan, Tashkent

PRACTICAL IMPLEMENTATION OF DOMAIN INFRASTRUCTURE FOR AN ENTERPRISE: FROM SERVER ENVIRONMENT PREPARATION TO SECURITY OPTIMIZATION

Abstract: *This article examines the comprehensive process of practical implementation of domain infrastructure for enterprises and organizations. The stages of server environment preparation, Domain Controller installation and configuration, DNS and DHCP services integration, as well as user account creation and security policy configuration are presented. Special attention is paid to backup and recovery, Defense-in-Depth protection, Tiered Administration model, and centralized security management through Group Policy. The research results can be applied in designing and deploying domain infrastructure in medium and large organizations.*

Keywords: *domain infrastructure, Active Directory, Domain Controller, Group Policy, security, DNS, DHCP, backup*

Современные предприятия и организации сталкиваются с необходимостью централизованного управления информационными ресурсами, пользователями и политиками безопасности. В условиях цифровизации бизнес-процессов доменная инфраструктура становится ключевым элементом корпоративной IT-архитектуры, обеспечивающим единую аутентификацию, авторизацию, аудит и контроль доступа. Несмотря на широкое распространение облачных технологий, локальная доменная инфраструктура на базе Active Directory продолжает оставаться основным инструментом управления в большинстве средних и крупных организаций [1, 2]. Целью данного исследования является комплексное

рассмотрение процесса практического внедрения доменной инфраструктуры — от подготовки серверной среды до оптимизации механизмов безопасности.

Подготовка серверной среды — это фундаментальный этап, от качества выполнения которого зависит стабильность и безопасность всей доменной инфраструктуры. Серверная среда представляет собой техническую и программную платформу, на которой функционируют доменные службы. Подготовка включает не только установку операционной системы, но и планирование аппаратных ресурсов, определение сетевых параметров, формирование политики безопасности, настройку механизмов резервирования и учёт масштабируемости в перспективе [3]. Практический опыт показывает, что множество проблем, возникающих при эксплуатации доменной инфраструктуры, связаны именно с ошибками, допущенными на этапе подготовки. Ключевыми требованиями к серверной среде являются: обеспечение высокой доступности (high availability) за счёт развёртывания нескольких Domain Controller, высокая производительность, достигаемая выделением достаточных вычислительных ресурсов, а также использование виртуализации для создания тестовых сред и быстрого восстановления серверов [4]. При выборе серверной операционной системы учитываются политика обновлений, наличие патчей безопасности, поддержка со стороны производителя и квалификация администраторов. В рамках практической реализации для серверов Domain Controller была выбрана операционная система Windows Server 2022 Standard. Для каждого контроллера домена были настроены статические IP-адреса, что является обязательным требованием для корректного функционирования доменных служб.

Установка и настройка Domain Controller (DC) является одним из наиболее критичных этапов внедрения доменной инфраструктуры. Domain

Controller — это сервер, выполняющий функции хранения данных каталога, аутентификации пользователей, применения политик безопасности и управления репликацией. Некорректная установка или настройка DC впоследствии приводит к проблемам безопасности, сбоям репликации и затруднениям в управлении [1, 5]. Перед установкой DC необходимо убедиться в готовности сервера: правильное имя хоста (hostname), обновлённая операционная система, установленные патчи безопасности. Особое внимание следует уделить настройке DNS, поскольку без корректно работающей службы DNS доменный контроллер не может быть обнаружен клиентскими компьютерами, возникают проблемы входа пользователей и нарушается репликация. В исследовании процесс установки DC включал добавление ролей Active Directory Domain Services и DNS Server, а также компонентов .NET Framework 3.5 и Group Policy Management через диспетчер серверов (Server Manager). После установки ролей сервер был повышен до Domain Controller с созданием нового леса с корневым доменом TATU.UZ [6]. При настройке были заданы пароль DSRM (Directory Services Restore Mode), интеграция с DNS и имя NetBIOS. Важным аспектом является распределение FSMO-ролей (Flexible Single Master Operations): Schema Master, Domain Naming Master, RID Master, PDC Emulator и Infrastructure Master — каждая из которых обеспечивает целостность данных, стабильность системы и точность репликации. Для обеспечения высокой доступности был развёрнут второй Domain Controller с настройкой репликации с основным DC. Рекомендуется наличие минимум двух контроллеров домена для распределения нагрузки и обеспечения непрерывности служб [7].

Служба DNS является «основным каталогом» доменной среды. В среде Active Directory без DNS практически ни одна служба не может функционировать полноценно, поскольку все контроллеры домена, службы и ресурсы обнаруживаются через DNS-записи. DNS выполняет

следующие функции: сопоставление доменных имён с IP-адресами, хранение сервисных записей (SRV records), обнаружение контроллеров домена, поддержка процессов репликации и поиск серверов Global Catalog [8]. При установке Active Directory осуществляется глубокая интеграция с DNS, при которой специальные SRV-записи обеспечивают подключение клиентских компьютеров к соответствующему контроллеру домена. Служба DHCP упрощает управление сетью путём автоматического распределения IP-адресов. В крупных организациях ручная настройка IP-адресов на тысячах устройств практически невозможна. DHCP автоматически предоставляет клиентам IP-адрес, маску подсети, шлюз по умолчанию и суффикс доменного имени. Это снижает количество IP-конфликтов, сокращает объём административной работы и обеспечивает быстрое расширение сети [9]. Интеграция DNS и DHCP требует особого внимания к вопросам безопасности. Для обеспечения непрерывности служб рекомендуется использовать не менее двух DNS-серверов с AD-интегрированными зонами и контролем репликации, а также DHCP failover с балансировкой нагрузки или Split Scope.

В доменной инфраструктуре учётные записи пользователей и политики безопасности играют ключевую роль в обеспечении защиты информационных ресурсов. Учётная запись пользователя (User Account) представляет собой цифровой идентификатор, через который определяются права доступа к системным ресурсам. Каждой учётной записи присваиваются имя входа, пароль, SID (Security Identifier), членство в группах и уровни разрешений [10]. При создании учётных записей необходимо соблюдать принцип минимальных привилегий (Least Privilege), при котором пользователь получает только те разрешения, которые необходимы для выполнения своих обязанностей. Управление на основе ролей (RBAC) позволяет назначать разрешения в соответствии с должностью. Стандартизация формата имён входа обеспечивает

единообразие и упрощает администрирование. Политика паролей должна включать требования сложности, запрет повторного использования предыдущих паролей и политику блокировки учётных записей после определённого числа неудачных попыток входа. Эти меры существенно снижают эффективность атак методом перебора (brute-force) и позволяют выявлять подозрительную активность [11]. Многофакторная аутентификация (MFA), сочетающая пароль и биометрическую проверку, обеспечивает дополнительный уровень защиты.

Резервное копирование (Backup) и восстановление (Recovery) являются стратегически важными процессами для обеспечения стабильной и непрерывной работы доменной инфраструктуры. Ключевыми объектами резервирования выступают: база данных Domain Controller, каталог Active Directory, зоны DNS, объекты Group Policy, папка SYSVOL и службы сертификатов [12]. В исследовании применялись три основных типа резервного копирования: полное (Full), инкрементальное (Incremental) и System State Backup — наиболее важный тип для Domain Controller, включающий базу данных Active Directory, SYSVOL, реестр и загрузочные файлы. В виртуализированной среде для DC предпочтительным является VM-level backup, тогда как использование снимков (snapshots) требует осторожности из-за возможных проблем с репликацией.

Для обеспечения безопасности доменной инфраструктуры была применена концепция многоуровневой защиты (Defense-in-Depth), включающая независимые уровни: физическая безопасность, сетевая безопасность, безопасность на уровне серверов, безопасность приложений, аутентификация пользователей и аудит [13]. Модель Tiered Administration разделяет административные привилегии на уровни (Tier 0 — управление идентификацией, Tier 1 — серверная инфраструктура, Tier 2 — рабочие станции), что предотвращает горизонтальное перемещение злоумышленников при компрометации учётной записи. Group Policy (GPO)

обеспечивает централизованное управление безопасностью доменной инфраструктуры. Через GPO применяются Security Baseline — минимальные наборы настроек безопасности, обязательные для всех серверов и рабочих станций. К основным мерам относятся: отключение неиспользуемых служб, ограничение USB-устройств, ограничение RDP-доступа, отключение функции AutoRun, блокировка неиспользуемых портов и настройка политик аудита [5, 14]. Комплексное применение описанных мер позволяет существенно повысить уровень безопасности доменной инфраструктуры и снизить риск реализации киберугроз [15].

Таким образом, практическое внедрение доменной инфраструктуры представляет собой многоэтапный процесс, требующий системного подхода на каждом этапе — от подготовки серверной среды и установки Domain Controller до настройки служб DNS и DHCP, управления учётными записями и оптимизации безопасности. Результаты исследования подтверждают, что корректное планирование и последовательная реализация каждого этапа обеспечивают стабильность, безопасность и управляемость доменной инфраструктуры, что имеет критическое значение для средних и крупных организаций.

Использованные источники:

1. Rand Morimoto, Jeffrey Shapiro. Active Directory: Designing, Deploying, and Running Active Directory. – Sybex, 2018.
2. Microsoft Corporation. Active Directory Domain Services Overview. – Microsoft Learn, 2022.
3. Limoncelli T., Hogan C., Chalup S. The Practice of System and Network Administration. – Addison-Wesley, 2016.
4. VMware Inc. vSphere Security Guide. – VMware Documentation, 2021.
5. Microsoft Corporation. Group Policy Fundamentals. – Microsoft Learn, 2021.
6. Minasi M. Mastering Windows Server 2019. – Wiley, 2019.

7. Microsoft Corporation. Active Directory Backup and Recovery Guide. – Microsoft Learn, 2022.
8. RFC 1034. Domain Names – Concepts and Facilities. – IETF, 1987.
9. RFC 2131. Dynamic Host Configuration Protocol (DHCP). – IETF, 1997.
10. Harwood M. Exam Ref 70-742 Identity with Windows Server. – Microsoft Press, 2018.
11. Scarfone K., Souppaya M. Guide to Enterprise Password Management. – NIST Special Publication 800-118, 2009.
12. Tulloch M. Microsoft Windows Server 2016 Administration Inside Out. – Microsoft Press, 2017.
13. NIST. Security and Privacy Controls for Information Systems and Organizations. – SP 800-53 Rev.5, 2020.
14. Kouti K., Seitsonen T. Active Directory Security Cookbook. – O'Reilly Media, 2020.
15. Microsoft Corporation. Securing Privileged Access Reference Material. – Microsoft Security, 2021.